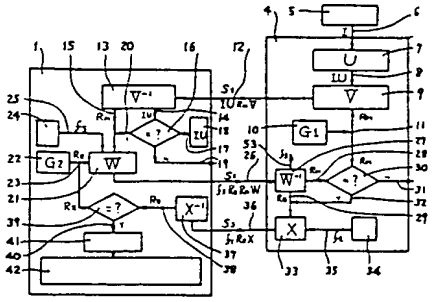
(54) IC CARD SYSTEM
(11) 63-184164 (A) (43) 29.7.198[redacted]9) JP
(21) Appl. No. 61-188186 (22) 11.8.1986
(71) HIKARI YOKOEKAWA (72) HIKARI YOKOEKAWA
(51) **Int. Cl⁴. G06F15/21,G06F15/30,G06K17/00**

PURPOSE: To decide the justifiability of a main device and a card, by sending a data including a random number from the main device side and the card side to an opponent side to each other, returning it to a transmission side after processing at the opponent side, and collating it with an original random number.

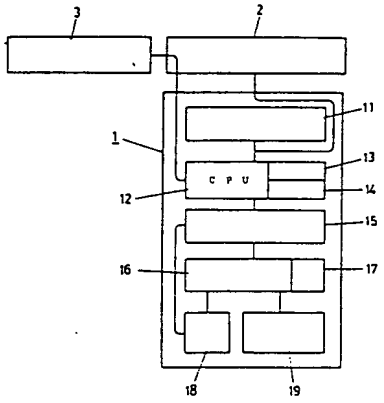
CONSTITUTION: At the main device 4, a signal IU converted from an inputted identification I at conversion U8 is sent to the random number R_M of a random number generator 10 and the card 1 converted at conversion V9. At the card 1, the signal IU and the random number R_M are recovered and separated at reverse conversion $V^{-1}13$, and at a collator 16, the signal IU is collated with the identification data of an identification data storage 18. When both coincide, the random numbers R_E and R_M of a random number generator 22 are converted at conversion W21, then, they are sent to the main device 4. At the main device 4, the random numbers R_M and R_E are recovered and separated at reverse conversion $W^{-1}27$, and the random number R_M is collated with the original random number R_M at a collator 30, and when they coincide, the random number R_E is converted at conversion X33, and is sent to the card 1. At the card 1, when the random number R_E recovered at revere conversion $X^{-1}37$ coincides with the original random number R_E, access to a memory zone 42 is permitted.



(54) PORTABLE PRODUCT DATA PROCESSOR
(11) 63-184165 (A) (43) 29.7.1988 (19) JP
(21) Appl. No. 62-15098 (22) 27.1.1987
(71) FUAMIRII MAATO K.K.(2) (72) HITOSHI SAKUMA(2)
(51) **Int. Cl⁴. G06F15/24,G06K7/10,G07G1/00**

PURPOSE: To easily perform the ordering and the stock control of a product, by providing a wand scanner which reads the product code of the product and a product data corresponding to the product code in a portable device.

CONSTITUTION: First of all, the product code read from the bar code of the product by the wand scanner 3 is inputted to the CPU12 of a main body 1, and the product data such as the product name, the optimum stock quantity, etc., of the product corresponding to the product code is read out from a file memory 15, and is displayed on a display part 11. At this time, by inputting a preset stock quantity from a keyboard 16, an ordering quantity is calculated from the data of the optimum stock quantity included in the product code and the data of the present stock quantity, and a calculated result (ordering quantity) is stored in the file memory 15. And after performing such work on every product, the ordering quantity of each product stored in the file memory 15 is printed out with a printer unit 2.

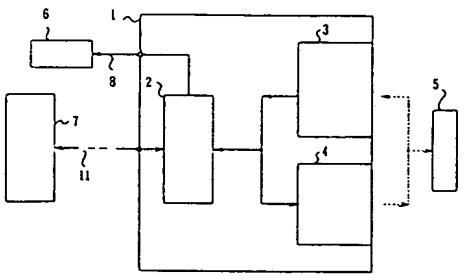


11: LCD display part, 13: OS memory, 14: program memory, 17: buzzer, 18: backup battery, 19: battery package

(54) AUTOMATIC REPAYMENT DEVICE FOR VOTING TICKET
(11) 63-184166 (A) (43) 29.7.1988 (19) JP
(21) Appl. No. 62-16724 (22) 27.1.1987
(71) FUJITSU LTD (72) YOICHI HIRASAWA
(51) **Int. Cl⁴. G06F15/28,G07D9/00**

PURPOSE: To prevent the exerciser of an unauthorized pari-mutuel ticket from escaping and to prevent the recurrence of malfeasance from occurring, by informing the fact of a repayment request by the unauthorized pari-mutuel ticket to a competition manager without being recognized by a repayment requesting person.

CONSTITUTION: When the repayment requesting person 5 inserts a pari-mutuel ticket to an automatic repayment device 1 for a voting ticket, the content of the ticket is read by a voting ticket processing part 3, and a read data is sent to a central processor 7 by a control part 2 via a communication line 11. The central processor 7 refers the described content of the pari-mutuel ticket to the result of a corresponding race, then, decides a refund money, however, when it is found that the pari-mutuel ticket is a forged or altered ticket, the information of the detection of the malfeasance is returned to the device 1. And the device 1 receiving the information of the detection of the malfeasance makes a money processing 4 operates as if normal repayment is performed to the repayment requesting person 5, and also, the information is sent with an alarm means 6 only recognizable by the competition manager.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－184164

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)7月29日
G 06 F 15/21	340	C－7230－5B	
15/30	340	7208－5B	
G 06 K 17/00		T－6711－5B	審査請求　未請求　発明の数 1　（全5頁）

㊹発明の名称　ICカードシステム

㉑特　願　昭61－188186
㉒出　願　昭61(1986)8月11日

㉒発明者　横江川　光　東京都足立区東綾瀬2－5－2－401
㉑出願人　横江川　光　東京都足立区東綾瀬2－5－2－401

明細書

1　発明の名称　ICカードシステム

2　特許請求の範囲

主装置が乱数R_M又はR_Mを含むデータをカードに送り，カードで加工ののち主装置に戻すα環状路と，カードが乱数R_E又はR_Eを含むデータを主装置に送り，主装置で加工ののちカードに戻すβ環状路を併設したICカードシステム。

3　発明の詳細な説明

本発明は，カードの改ざんや偽造，主装置の不正作成使用を防止するICカードシステムに関する。従来のICカードシステムでは，使用中のカード端子から盗聴等で得た信号を記録し，のちにこの信号を再利用する不正使用への対策がなかった。本発明は，ICカードシステムに，主装置が乱数R_M又はR_Mを含むデータをカードに送り，カードで加工ののち主装置に戻すα環状路と，カードが乱数R_E又はR_Eを含むデータを主装置に送り，主装置で加工ののちカードに戻すβ環状路を併設する。たとえば，主装置に発生させた乱数R_Mを変換又は少くともR_Mを含む1組の値を合体変換した信号S_1をカードへ送り，カードがS_1から復元したR_M又は復元R_Mにもとづく変換値を信号S_2又はS_2'として主装置に返送し，さらにカード内にて発生させた乱数R_Eを変換又は少くともR_Eを含む1組の値を合体変換した信号S_2又はS_2''を主装置へ送り，主装置が，復元したR_E又は復元R_Eにもとづく変換値を信号S_3としてカードに返送する，ICカード，主装置，およびそれらより成るICカードシステムを構成する。

α環状路は，主装置からカードに信号S_1を送る往路と，カードから主装置に信号S_2'を返す復路と，β環状路は，カードから主装置に信号S_2''を送る往路と，主装置からカードに信号S_3を返す復路を持つ。αとβを独立に構成する他，S_2'とS_2''をS_2にまとめた，一部共有の構成も可能である。

β環状路の復路信号S_3を用いた照合結果にてメモリゲート駆動を行う構成とする。また，α環状路についてはカード内にて行う変換処理の結果が，β環状路については主装置内にて行う変換処理の

結果が，それぞれ反映される復路信号とする．よって，復路信号を往路信号と異るデータ形式に構成する。さらに，信号に複数の情報を混載しうる。例えば往路の往路信号S_1にて，乱数R_Mの他に暗証Iやその変換IUはじめ，パスワードやファイルキー，口座番号などfコードを混載できる。この際送信中の盗聴解読防止のため，複数の情報の合体変換加工を行う。ある環状路で運んだf等を，他の環状路に入力して処理，照合，同期等に用いる構成も可能である。

第1図は本発明のICカードシステム構成図にて，少くともIC外部からのアクセス不能のメモリ⑫や制御プログラム⑬とCPU⑭をもつ主回路①を設置した，端子⑮つきICカード②及び，当該ICカードとの読出し書込み及びデータ処理を行う主装置③より，ICカードシステムが構成される。主回路①は，ワンチップIC又は数個のICにて実現する。主装置③は，少くとも外部からのアクセス不能メモリ㊶や制御プログラム㊷とCPU㊸をもつ主回路④を搭載する。主回路④はワンチップICや複数個のICをアセンブルしてブラックボックス化した集合体にて実現する他，主回路の代用として別のICカードを組込んで用いることもできる。

第2図は，本発明の実施例の処理の流れを示す。キー入力器⑤より入力の暗証I⑥を変換U⑦にてIU⑧に変換ののち変換T⑨に入力する。⑨は主装置内の乱数発生器G_1⑩で発生させた乱数R_M⑪とIU⑧とを合体変換加工して信号S_1⑫をつくり，カードに送る。S_1のフォーマットをIUR_MTにて示す。IUとR_Mの順序は任意でよい。カード内にて，逆変換T^{-1}⑬が復元IU⑭と復元R_M⑮を復元分離する。照合器⑯は⑭と，識別データ格納器⑰より取出した識別データIU⑱を比較照合し，不合致⑲なら排除し，合致⑳なら使用者と主装置が正当と判定して⑮を変換W㉑に送るのを許可する。㉑はカード内の乱数発生器G_2㉒で発生させた乱数R_E㉓と，f_S格納器㉔から取出したコードf_S㉕とを合体変換加工して信号S_2㉖をつくり，主装置に送る。S_2のフォーマットを$f_S R_E R_M$Wにて示す。f_S，R_E，R_Mの順序は任意でよく，またf_Sは省略してもよい。主装置内にて，逆変換W^{-1}㉗が復元R_M㉘と復元R_E㉙を復元分離する。照合器㉚は㉘と，もとの乱数R_M⑪を比較照合し，不合致㉛なら排除し，合致㉜ならカードを正当と判断して㉙を変換X㉝に送るのを許可する。㉝は㉙と，f_1格納器㉞より取出したコードf_1㉟とを合体変換加工して信号S_3㊱をつくり，カードに送る。S_3のフォーマットを，$f_1 R_E$Xにて示す。f_1，R_Eの順序は任意でよく，またf_1は省略もできる。

カード側にて，逆変換X^{-1}㊲がS_3㊱から復元R_E㊳を分離し．照合器㊴にて㊳と，もとの乱数R_E㉓を比較照合の上，合致㊵すればメモリゲート㊶をオープンし，メモリゾーン㊷へのアクセスを許可する。

このように，カード側の照合器⑯にて復元IU⑭を検査するので使用者と主装置の両方の正当性をカードが判定でき，一方主装置側では，もとのR_Mに対し主装置及びカードにて変換と逆変換をくり返した結果に得るR_Mを主装置に還流させ，もとのR_Mと比較照合することで，カードの正当性を判定できる。

上記にて，もしカード内で発生させた乱数R_Eを用いず，主装置がカードにR_Eを含まぬ信号S_3を送る構成とすると，信号の盗聴再利用を許してしまい不都合である．たとえばカードを正常使用中に端子からS_2とS_3信号を盗聴記録しておき，のちに正当でない主装置を用いて盗聴したS_2信号をカードに入力すれば不正にカードを起動でき，カードより送られるS_2やS_3信号をよみとばして，盗聴したS_3信号を入力すれば，不正の主装置にてメモリへのアクセスを可能としてしまい，他人や自分自身のカードの額面改ざん等を可能としてしまう。

そこで，カードにてR_Eを発生させ，R_E又は少くともR_Eを含む値の変換値をカードから主装置に送り，主装置は受けたR_Eの変換値又は少くともR_Eを含む値の変換値を信号S_3としてカードに返送し，カードにて復元したR_Eを，もとの発信したR_Eと比較

照合して合致時にのみメモリゲートをオープンするよう構成すれば，主装置がたしかにカードから先刻発信されたReにもとづきS3を作成したと確認できる。よって，盗聴しておいたS3をカード入力しても，使用したRe値がその都度異るため，照合は成立せず，メモリアクセスできない。即ち，信号の盗聴再利用を防止できる。

合体変換する信号は，送信途上での盗聴解読防止のためであり，さらに複数個のデータをからみあわせて送ることで互にカムフラージュすると共に一度に送信できるゆえ，カードと主装置間の送受信回数を減少できる。合体変換した結果のフォーマット，例えば fs Re Rm W という表示は，fsやRe，Rmといったコードや値を，手順Wを用いて変換処理した出力を示す。一例として

fs　01010011
Re　11010110
Rm　10101110

とし，W手順を

① fsをビット反転
② Reの上4ビットと，①を施したfsの下4ビットを交換
③ Rmの上4ビットと，Reの下4ビットを交換
④ Rmの下4ビットと，①を施したfsの上4ビットを交換
⑤ 以上の順にてできた3バイトを合体して信号S2となす

とすれば，S2は 16進表示で EDCA6A が生成される。さらに，fsのバイト数を増加させ，秘密度を高めうる。又，W⁻¹手順は，上記W手順の逆プロセスとなる。

主装置に設けた変換Uは，主装置が不正目的で盗まれたり，秘密が洩れた時の暗号更新を円滑に行うための構成で，主装置を更新する際は変換U⑦を更新するのみでよい。カード使用者には，必ず本人確認ののち，入力されたIをもとに新IUを作成して識別データ格納器⑱を更新するのみでよい。

fには，パスワード，ファイルアクセスキーや其他任意の値，コードを採用しうる。

識別データとしてIUのかわりにパスワード等fiを暗証入力Iと組合せて用いる際は，第3図に示すように構成し，信号S1のフォーマットを fi I Rm V とすればよい。

第4図に信号のフォーマット例を示す。第4図(a)にてS1のフォーマットは fi IU Rm V あるいは fi I Rm V，S2'のそれは f3 Rm W となる。W=V，f3=fiも可能である。S2"のそれは f2 Re あるいは f2 Re Y となり，Yは変換を示す。Y=V，Y=Wも可能である。f2は省略できる。

S3のフォーマットは f1 Re X であり，f1は省略できる。

第4図(b)は，ReとRmをひとつの信号内に組込む構成の例で，S1，S3のフォーマットは第4図(a)と同じであるが，S2のそれは fs Re Rm W となる。W=V，fs=fs も可能である。

51がα環状路，52がβ環状路を示す。

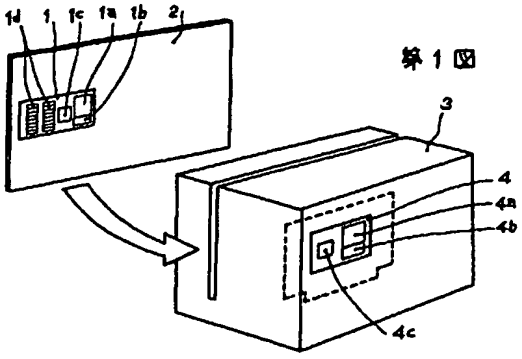
53は運送し復元したfs，例えば口座番号等である。

4 図面の簡単な説明

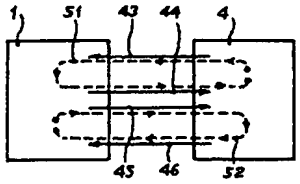
第1図は本発明のカードシステムの構成図，第2図と第3図は実施例の処理のながれを，第4図は信号のフォーマットを示す。

1…カードの主回路，1a…外部からアクセス不能メモリ，1b…制御プログラム，1c…CPU，1d…端子，2…ICカード，3…主装置，4…主装置の主回路，4a…外部からアクセス不能メモリ，4b…制御プログラム，4c…CPU，5…キー入力器，6…暗証I，7…変換U，8…IU，9…変換V，10…乱数発生器G1，11…乱数Rm，12…信号S1，13…逆変換V⁻¹，14…復元IU，15…復元Rm，16…照合器，18…識別データ格納器，17…識別データIU，19…不合致，20…合致，21…変換W，22…乱数発生器G2，23…乱数Re，24…fs格納器，25…コードfs，26…信号S2，27…逆変換W⁻¹，28…復元Rm，29…復元Re，30…照合器，31…不合致，32…合致，33…変換X，34…f2格納器，35…コードf2，

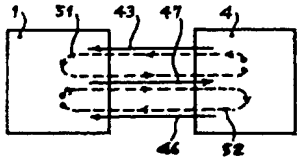
36…信号S_3，37…逆写像X^{-1}，38…復元R_E，
39…照合器，40…合致，41…メモリゲート，
42…メモリゾーン，43…信号S_1，49…信号S_2'，
45…信号S_2''，46…信号S_3，47…信号S_2，
48…f_4格納器，49…コードf_4，50…信号S_1
51…α環状路，52…β環状路
53…復元f_5



第1図

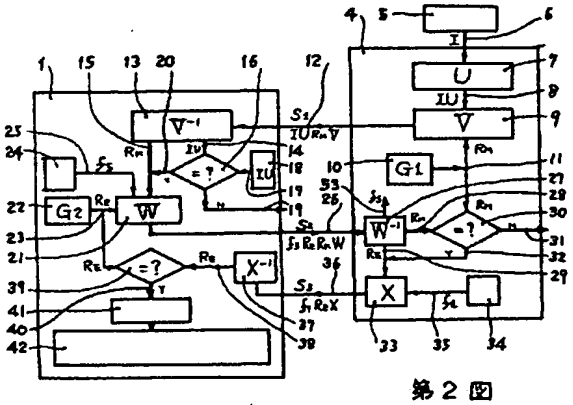


第4図
〔a〕

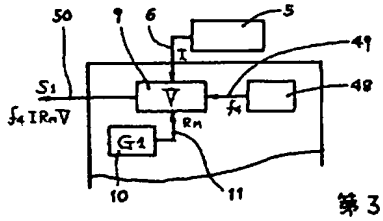


〔b〕

特許出願人　横江川　光



第2図



第3図

手続補正書

昭和62年11月10日

特許庁長官　殿
(~~特許庁審査官~~　殿)

1. 事件の表示
昭和61年　特許願第188186号

2. 発明(~~考案~~)の名称(フリガナ)　ICカードシステム
~~意匠に係る物品~~
~~指定商品および商品の区分~~
~~第　類~~

3. 補正をする者
事件との関係　特許出願人
住所　郵便番号 120-00
東京都足立区東綾瀬2-5-2-401
氏名(フリガナ)(法人にあっては名称および代表者の肩書を含めてその代表者)　横江川　光

~~4. 補正命令の日付　昭和　年　月　日~~

5. 補正の対象
明細書の発明の詳細な説明の欄

6. 補正の内容
別紙のとおり

補正の内容

1　オ8頁　オ19行目
「 f_5には，」　とあるを，
「 f_1 や f_5 などには，」 に補正。

2　オ10頁　オ20行目
「 3f… f_2 格納番 」 とあるを，
「 3f… f_1 格納番 」 に補正。

3　オ8頁　オ20行目の後に以下を挿入。
「
いまS1とS2の往復にて，主装置と使用者が正当と確定できたとして，例えばカードのメモリゾーン㊷にデータをかきこみたいとき，カード側に書込みを告げるコード f_1㉟を用いるが，このとき対象のアドレスや書込むべきデータなどを f_1 に添え又は連結して f_1' となし，f_1' R_E X のフォマットのS3をカードに送り，カードが X^{-1}㊲にて R_E㊳を復元時に f_1' も復元しておき，R_E 照合合致㊵ののち f_1' を処理して書込みを実行させればよい。このとき，複数個のS3を発信することを告げる f_1 を用いたS3を1個，先ず発信し，ついでデータを f_1 としてのせたS3を告げた個数だけカードに送ることにて，多量のデータを一挙にカードに送りこめる。
カード側にて書込みが正常に完了すれば，それを通知するコード f_5 を再びS2の発信にて，主装置側に通知することもできる。即ち，信号のやりとりはS1，S2，S3，S2と続き，このようにα環状路とβ環状路を何度もくり返して交信ができる。この一連の交信時に，同一の R_M や R_E を用いてもよく，又例えば1回の交信毎に異った乱数を用いてもよい。このとき，S3のフォマットとしてS2のフォマットと類似の f_1 R_E R_M X を用いれば，1回毎に異る乱数によるα，β両環状路の連続交信が可能になる。カードのメモリゾーン㊷からの多量データよみ出しも，このαβの連続にて授受できる。 」

手続補正書

昭和63年3月1日

特許庁長官　殿
（特許庁審査官　殿）

1. 事件の表示
昭和61年　特許　願　第188186号

2. 発明（考案）の名称　ICカードシステム

3. 補正をする者
事件との関係　特許　出願人
住所　郵便番号 160-00
東京都足立区東綾瀬2-5-2-401
03-604-7103
氏名（法人にあっては名称および代表者の姓を続けてその氏名）　横江川

4. 補正命令の日付　昭和63年2月2日

5. 補正により増加する請求項の数

6. 補正の対象　昭和62年11月10提出の手続補正書の「補正の対象」の欄

7. 補正の内容　別紙のとおり

特許 63.3.1 正版

手続補正書

昭和62年11月10日

特許庁長官　殿
（特許庁審査官　殿）

1. 事件の表示
昭和61年　特許　願　第188186号

2. 発明（考案）の名称　ICカードシステム

3. 補正をする者
事件との関係　特許　出願人
住所　郵便番号 160-00
東京都足立区東綾瀬2-5-2-401
氏名（法人にあっては名称および代表者の姓を続けてその氏名）　横江川

4. 補正命令の日付　昭和　年　月　日

5. 補正により増加する請求項の数

6. 補正の対象　明細書の発明の詳細な説明の欄
明細書の図面の簡単な説明の欄

7. 補正の内容　別紙のとおり